Etude du mécanisme «Certificate Transparency » et de son impact à court terme

Auteurs

Hassen NASRI
Thierno LO

Encadreurs

Maryline LAURENT (TSP)
Jean Michel COMBES (Orange)

Partenaires

Objectifs du mécanisme

Standardisé sous le RFC6962 par l'IETF, propulsé et mise en œuvre par Google

Le mécanisme CT a pour objectif de :

- Rendre difficile (voir impossible) l'émission de certificats X.509 par les AC pour un domaine (site internet) à l'insu de son propriétaire
- Fournir un système d'audit et de monitoring public qui permettra à tout propriétaire de domaine de vérifier l'état d'émission d'un certificat (sûr ou frauduleux)
- Protéger l'utilisateur final des attaques liées à l'utilisation de certificats malicieux ou volés

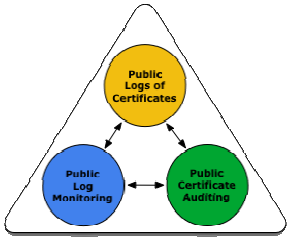


Figure 1: Les composants de Certificate Transparency http://www.certificate-transparency.org/_/rsrc/1375725320520/what-is-ct/ct_intro_system.png

Caractéristiques et fonctionnement

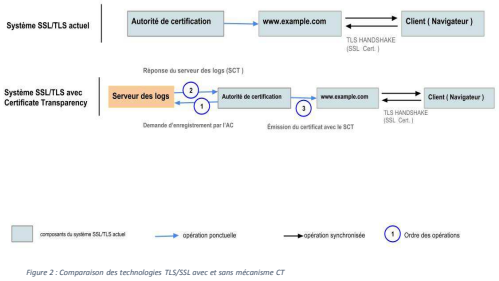


Figure 2 : Comparaison des technologies TLS/SSL avec et sans mécanisme CT

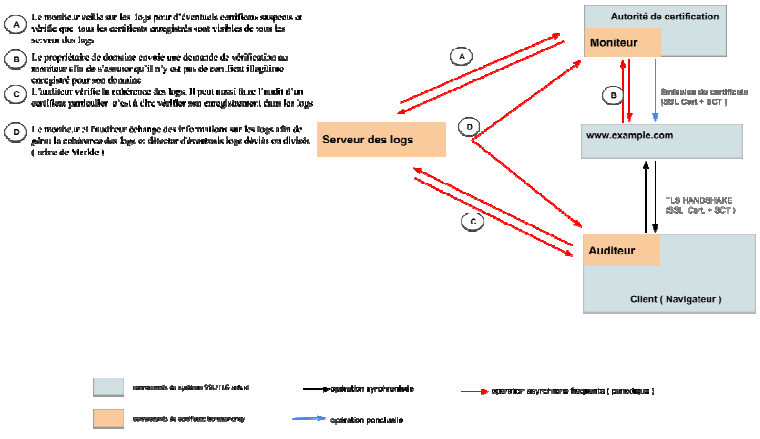
Ce principe est implémenté sur un système d'audit et monitoring ouvert des certificats TLS/SSL (figure1) et il est composé

- **Serveur de logs :** service réseau permettant de garder la traçabilité des certificats émis
- **Moniteur :** serveurs publics qui, périodiquement, analysent les logs des certificats(serveur des logs) et signalent les certificats suspects.
- **Auditeur :** composants logiciels légers qui exécutent deux fonctions :
  - La vérification des logs (intégrité et cohérence des entrées)
  - La présence d'un certificat particulier

Impact sur le système actuel

- Traçabilité des émissions de certificats
- Transparence des certificats
- Application sur 6% des sites internet (janvier) et 75%(juillet 2015)
- Pouvoir de décision aux propriétaires de domaine
- Nouvelles offres de services pour les AC

Configuration typique du mécanisme



Projet de fin d'études – VAP Sécurité des systèmes et des réseaux

Janvier 2015

Contact thierno.lo@telecom-sudparis.eu
hassen.nasri@telecom-sudparis.eu

Site web : www.telecom-sudparis.eu